Implementar funciones e integraciones

BeeGFS on NetApp with E-Series Storage

NetApp
January 27, 2026

This PDF was generated from https://docs.netapp.com/es-es/beegfs/deploy-features-integration/beegfs-csi-driver/csi-driver-overview.html on January 27, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Implementar funciones e integraciones

Controlador CSI de BeeGFS

Configura el cifrado TLS para BeeGFS v8

Configura el cifrado TLS para proteger la comunicación entre los servicios de gestión de BeeGFS v8 y los clientes.

Descripción general

BeeGFS v8 introduce la compatibilidad con TLS para cifrar las comunicaciones de red entre herramientas administrativas (como la utilidad de línea de comandos `beegfs`) y servicios de servidor BeeGFS como Management o Remote. Esta guía cubre cómo configurar el cifrado TLS en tu clúster BeeGFS usando tres métodos de configuración TLS:

- **Usar una autoridad de certificación de confianza:** Usa los certificados firmados por CA existentes en tu clúster BeeGFS.
- **Crear una Autoridad de Certificación local:** Crear una Autoridad de Certificación local y usarla para firmar certificados para tus servicios BeeGFS. Este enfoque es adecuado para entornos donde quieres gestionar tu propia cadena de confianza sin depender de una CA externa.
- **TLS Disabled:** deshabilita TLS por completo para entornos donde no se requiera cifrado o para la resolución de problemas. Esto se desaconseja ya que expone información potencialmente sensible sobre la estructura interna del sistema de archivos y la configuración como texto claro.

Elige el método que mejor se adapte a tu entorno y políticas organizativas. Consulta la "BeeGFS TLS" documentación para más detalles.

> Las máquinas que ejecutan el `beegfs-client` servicio no necesitan TLS para montar el sistema de archivos BeeGFS. TLS debe configurarse para utilizar la BeeGFS CLI y otros servicios beegfs, como remote y sync.

Uso de una autoridad de certificación de confianza

Si tienes acceso a certificados emitidos por una autoridad de certificación (CA) de confianza, ya sea de una CA interna de la empresa o de un proveedor externo, puedes configurar BeeGFS v8 para usar estos certificados firmados por la CA en vez de generar certificados autofirmados.

Implementar un nuevo clúster BeeGFS v8

Para un nuevo despliegue de clúster BeeGFS v8, configura el archivo `user_defined_params.yml` del inventario de Ansible para que haga referencia a tus certificados firmados por CA:

```
beegfs_ha_tls_enabled: true

beegfs_ha_ca_cert_src_path: files/beegfs/cert/ca_cert.pem

beegfs_ha_tls_cert_src_path: files/beegfs/cert/mgmtd_tls_cert.pem

beegfs_ha_tls_key_src_path: files/beegfs/cert/mgmtd_tls_key.pem
```

> Si `beegfs_ha_tls_config_options.alt_names` no está vacío, Ansible generará automáticamente un certificado y una clave TLS autofirmados usando los alt_names proporcionados como Subject Alternative Names (SANs) en el certificado. Para usar tu propio certificado y clave TLS personalizados (como se especifica en `beegfs_ha_tls_cert_src_path` y `beegfs_ha_tls_key_src_path`), tienes que comentar o eliminar toda la sección `beegfs_ha_tls_config_options`. De lo contrario, la generación del certificado autofirmado tendrá prioridad y tu certificado y clave personalizados no se usarán.

Configurar un clúster BeeGFS v8 existente

Para un clúster BeeGFS v8 existente, establece las rutas en el archivo de configuración de los servicios de gestión de BeeGFS a los certificados firmados por CA del nodo de archivos:

```
tls-cert-file = /path/to/cert.pem
tls-key-file = /path/to/key.pem
```

Configurar clientes BeeGFS v8 con certificados firmados por CA

Para configurar los clientes de BeeGFS v8 para que confíen en certificados firmados por CA usando el grupo de certificados del sistema, establece tls-cert-file = '' en la configuración de cada cliente. Si no se está usando el grupo de certificados del sistema, proporciona la ruta a un certificado local estableciendo tls-cert-file = <local cert>. Esta configuración permite que los clientes autentiquen los certificados presentados por los servicios de gestión de BeeGFS.

Creando una autoridad de certificación local

Si tu organización quiere crear su propia infraestructura de certificados para el clúster BeeGFS, puedes crear una autoridad de certificación (CA) local para emitir y firmar certificados para tu clúster BeeGFS. Este enfoque implica crear una CA que firme certificados para los servicios de gestión de BeeGFS, los cuales luego se distribuyen a los clientes para establecer una cadena de confianza. Sigue estas instrucciones para configurar una CA local y desplegar certificados en tu clúster BeeGFS v8 existente o nuevo.

Implementar un nuevo clúster BeeGFS v8

Para un nuevo despliegue de BeeGFS v8, el rol de `beegfs_8` Ansible se encargará de crear una CA local en el nodo de control y de generar los certificados necesarios para los servicios de gestión. Esto puede habilitarse configurando los siguientes parámetros en el archivo de inventario de Ansible `user_defined_params.yml`:

```
beegfs_ha_tls_enabled: true

beegfs_ha_ca_cert_src_path: files/beegfs/cert/local_ca_cert.pem

beegfs_ha_tls_cert_src_path: files/beegfs/cert/mgmtd_tls_cert.pem

beegfs_ha_tls_key_src_path: files/beegfs/cert/mgmtd_tls_key.pem

beegfs_ha_tls_config_options:
  alt_names: [<mgmt_service_ip>]
```

Si `beegfs_ha_tls_config_options.alt_names` no se proporciona, entonces Ansible intentará usar los certificados existentes en las rutas de certificado/clave especificadas.

Configurar un clúster BeeGFS v8 existente

Para un clúster BeeGFS existente, puedes integrar TLS creando una autoridad de certificación local y generando los certificados necesarios para los servicios de gestión. Actualiza las rutas en el archivo de configuración de los servicios de gestión de BeeGFS para que apunten a los certificados recién creados.

Las instrucciones de esta sección son para que las uses como referencia. Debes tomar las precauciones de seguridad adecuadas al manejar claves privadas y certificados.

Crear la autoridad de certificación

En un equipo de confianza, crea una Autoridad de Certificación local para firmar certificados para tus servicios de gestión de BeeGFS. El certificado CA se distribuirá a los clientes para establecer confianza y permitir una comunicación segura con los servicios de BeeGFS.

Las siguientes instrucciones son una referencia para crear una Autoridad de Certificación local en un sistema basado en RHEL.

1. Instala OpenSSL si aún no está instalado:

```
dnf install openssl
```

2. Crea un directorio de trabajo para guardar los archivos de certificados:

```
mkdir -p ~/beegfs_tls && cd ~/beegfs_tls
```

3. Genera la clave privada de la CA:

```
openssl genrsa -out ca_key.pem 4096
```

4. Crea un archivo de configuración de CA llamado `ca.cnf` y ajusta los campos de nombre distintivo para

que coincidan con tu organización:

```
[ req ]
default_bits        = 4096
distinguished_name = req_distinguished_name
x509_extensions     = v3_ca
prompt              = no

[ req_distinguished_name ]
C  = <Country>
ST = <State>
L  = <City>
O  = <Organization>
OU = <OrganizationalUnit>
CN = BeeGFS-CA

[ v3_ca ]
basicConstraints = critical,CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
```

5. Genera el certificado CA. Este certificado debe ser válido durante toda la vida del sistema, de lo contrario tendrás que planear regenerar los certificados antes de que caduquen. Una vez que un certificado caduca, la comunicación entre algunos componentes no será posible y actualizar los certificados TLS normalmente requerirá reiniciar los servicios para completar el proceso.

   El siguiente comando genera un certificado CA válido por 1 año:

   ```
   openssl req -new -x509 -key ca_key.pem -out ca_cert.pem -days 365
   -config ca.cnf
   ```

   Aunque en este ejemplo se utiliza un periodo de validez de 1 año para simplificar, deberías ajustar el parámetro `-days` según los requisitos de seguridad de tu organización y establecer un proceso de renovación de certificados.

Crear certificados de servicio de administración

Genera certificados para tus servicios de gestión de BeeGFS y fírmales con la CA que creaste. Estos certificados se instalarán en los nodos de archivos que ejecutan servicios de gestión de BeeGFS.

1. Genera la clave privada del servicio de gestión:

   ```
   openssl genrsa -out mgmtd_tls_key.pem 4096
   ```

2. Crea un archivo de configuración de certificados llamado `tls_san.cnf` con Subject Alternative Names

(SANs) para todas las direcciones IP de los servicios de gestión:

```
[ req ]
default_bits       = 4096
distinguished_name = req_distinguished_name
req_extensions     = req_ext
prompt             = no

[ req_distinguished_name ]
C  = <Country>
ST = <State>
L  = <City>
O  = <Organization>
OU = <OrganizationalUnit>
CN = beegfs-mgmt

[ req_ext ]
subjectAltName = @alt_names

[ v3_ca ]
subjectAltName = @alt_names
basicConstraints = CA:FALSE

[ alt_names ]
IP.1 = <beegfs_mgmt_service_ip_1>
IP.2 = <beegfs_mgmt_service_ip_2>
```

Actualiza los campos de nombre distintivo para que coincidan con la configuración de tu CA y los valores `IP.1` y `IP.2` con las direcciones IP de tu servicio de gestión.

3. Genera una solicitud de firma de certificado (CSR):

```
openssl req -new -key mgmtd_tls_key.pem -out mgmtd_tls_csr.pem -config
tls_san.cnf
```

4. Firma el certificado con tu CA (válido por 1 año):

```
openssl x509 -req -in mgmtd_tls_csr.pem -CA ca_cert.pem -CAkey
ca_key.pem -CAcreateserial -out mgmtd_tls_cert.pem -days 365 -sha256
-extensions v3_ca -extfile tls_san.cnf
```

Ajusta el periodo de validez del certificado (`-days 365` según las políticas de seguridad de tu organización. Muchas organizaciones requieren la rotación de certificados cada 1-2 años.

5. Verifica que el certificado se haya creado correctamente:

```
openssl x509 -in mgmtd_tls_cert.pem -text -noout
```

   Confirma que la sección Nombre alternativo del asunto incluye todas tus direcciones IP de gestión.

Distribuye certificados a los nodos de archivos

Distribuye el certificado CA y los certificados del servicio de gestión a los nodos de archivos y clientes adecuados.

1. Copia el certificado de CA y el certificado y la clave del servicio de gestión en los nodos de archivos que ejecutan los servicios de gestión:

```
scp ca_cert.pem mgmtd_tls_cert.pem mgmtd_tls_key.pem
user@beegfs_01:/etc/beegfs/
scp ca_cert.pem mgmtd_tls_cert.pem mgmtd_tls_key.pem
user@beegfs_02:/etc/beegfs/
```

Apunta el servicio de gestión a los certificados TLS

Actualiza la configuración del servicio de gestión de BeeGFS para habilitar TLS y referenciar los certificados TLS creados.

1. Desde un nodo de archivos que ejecuta el servicio de gestión BeeGFS, edita el archivo de configuración del servicio de gestión, por ejemplo en `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml`. Agrega o actualiza los siguientes parámetros relacionados con TLS:

```
tls-disable = false
tls-cert-file = "/etc/beegfs/mgmtd_tls_cert.pem"
tls-key-file = "/etc/beegfs/mgmtd_tls_key.pem"
```

2. Toma las medidas necesarias para reiniciar de forma segura el servicio de gestión BeeGFS para que los cambios surtan efecto:

```
systemctl restart beegfs-mgmtd
```

3. Verifica que el servicio de gestión se inició correctamente:

```
journalctl -xeu beegfs-mgmtd
```

   Busca entradas de registro que indiquen una inicialización TLS exitosa y la carga de certificados.

```
Successfully initialized certificate verification library.
Successfully loaded license certificate: TMP-XXXXXXXXXX
```

Configura TLS para clientes BeeGFS v8

Crea y distribuye certificados firmados por la CA local a todos los clientes BeeGFS que necesiten comunicación con los servicios de gestión BeeGFS.

1. Genera un certificado para el cliente usando el mismo proceso que el certificado del servicio de gestión de arriba, pero con la dirección IP o el nombre de host del cliente en el campo Subject Alternative Name (SAN).
2. Copia de forma segura y remota el certificado del cliente al cliente y cambia el nombre del certificado a `cert.pem` en el cliente:

```
scp client_cert.pem user@client:/etc/beegfs/cert.pem
```

3. Reinicia el servicio cliente BeeGFS en todos los clientes:

```
systemctl restart beegfs-client
```

4. Verifica la conectividad del cliente ejecutando un comando `beegfs CLI` como:

```
beegfs health check
```

Desactivar TLS

TLS puede deshabilitarse para la resolución de problemas o si los usuarios así lo desean. Esto se desaconseja porque expone información potencialmente sensible sobre la estructura interna del sistema de archivos y la configuración en texto claro. Sigue estas instrucciones para deshabilitar TLS en tu clúster BeeGFS v8 existente o nuevo.

Implementar un nuevo clúster BeeGFS v8

Para una nueva implementación de clúster BeeGFS, el clúster se puede implementar con TLS deshabilitado configurando el siguiente parámetro en el archivo de inventario de Ansible `user_defined_params.yml`:

```
beegfs_ha_tls_enabled: false
```

Configurar un clúster BeeGFS v8 existente

Para un clúster BeeGFS v8 existente, edita el archivo de configuración del servicio de gestión. Por ejemplo, edita el archivo en `/mnt/mgmt_tgt_mgmt01/mgmt_config/beegfs-mgmtd.toml` y establece:

```
tls-disable = true
```

Toma las medidas necesarias para reiniciar de forma segura el servicio de gestión para que los cambios surtan efecto.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.